Application No. 1997-0051503
Laid-open No. 1999-0030989

Abstract

The present invention relates to a certification process method of a certification process apparatus, which protects a company from economical loss by issuing a certification key to a subscriber when he signs up for the service, conducting certification by using the issued certification key during the service and detecting an illegal subscriber or an illegal terminal. This invention can also protect the privacy of a subscriber as it prevents illegal wiretapping, and with its function of inspecting security polity, it can manage diverse forms of securities in general. Moreover, the present invention minimizes the effect of a load on a network by conducting certification, and it can be easily converted into a security polity device or into an inspection device by separating the certification request process device and the inspection device.

(19) 대한민국특허청(KR)
(12) 공개특허공보(A)

(51)°Int. Cl. 6 H04L 9 /00

(11) 공개번호 특1999-0030989
(43) 공개일자 1999년05월06일

(21) 출원번호 10-1997-0051503
(22) 출원일자 1997년10월08일

(71) 출원인 한국전기통신공사 이계철
경기도 성남시 분당구 정자동 206

(72) 발명자 박등국
경기도 성남시 분당구 구미동 12번지 건영빌라 501등 201호

오미나
서울특별시 은평구 역촌2동 54-15

정원영
경기도 과천시 주암동 63-10

김태근
경기도 안양시 동안구 갈산동 샘마을 119-901

(74) 대리인 이정훈, 이권희

심사청구 : 있음

(54) 인증처리 장치에서의 인증처리 방법

요약

본 발명은 인증처리 장치에서의 인증처리 방법에 관한 것으로, 서비스 가입시에 가입자에게 인증키를 할당하고, 서비스 제공시에 할당된 인증키를 사용하여 인증을 수행하여, 불법 가입자 및 불법 단말기를 검출하므로써 사업자의 경제적 손실을 차단하는 잇점이 있고, 불법 도청을 방지하므로써 가입자의 프라이버시 보호 잇점이 있으며, 보안정책 감사 기능을 통하여 다양한 형태의 보안 관리를 총괄적으로 수행할 수 있는 장점이 있고, 인증 수행으로 인해 망 부하에 주는 영향을 최소화 할 수 있는 잇점이 있으며, 인증요구 처리 장치를 보안정책 및 감사 장치와 분리시키므로써, 사업자가 원하는 보안정책 및 감사장치로의 변경이 용이한 잇점을 수반하는 기술이다.

대표도

도5

명세서

도면의 간단한 설명

도 1은 본 발명이 적용되는 개인통신 서비스망 기능 구조를 나타내는 도면.

도 2는 본 발명에 의한 인증방식을 개략적으로 설명하는 도면.

도 3은 본 발명에 의해 구현된 인증처리 장치 구성 블럭도.

도 4는 도 3에 도시된 인증요구처리부의 내부 상세 블럭도.

도 5는 본 발명에 의한 인증처리 방법 중 분배처리 기능의 실행 과정을 나타내는 순서도.

도 6은 본 발명에 의한 인증처리 방법 중 인증처리 기능의 실행 과정을 나타내는 순서도.

도 7은 본 발명에 의한 인증처리 방법 중 인증실패처리 기능의 실행 과정을 나타내는 순서도.

도 8은 본 발명에 의한 인증처리 방법 중 인증상태관리 기능의 실행 과정을 나타내는 순서도.

도 9는 본 발명에 의한 인증처리 방법 중 망인증처리 기능의 실행 과정을 나타내는 순서도.

도 10은 본 발명에 의한 인증처리 방법 중 인증상태 변경 기능의 실행 과정을 나타내는 순서도.

도 11은 본 발명에 의한 인증처리 방법 중 인증관련처리 트래픽 수집 기능의 실행 과정을 나타내는 순서도.

< 도면의 주요부분에 대한 부호의 설명 >

100 : 인증처리 장치 200 : 단말기

300 : 기지국/기지국 제어기

400 : 교환기/방문자 정보처리 시스템

500 : 가입자 정보처리 시스템 600 : 가입자 관리 시스템

10 : 가입자 정보처리 시스템 접속부

11 : 인증요구 처리부 110 : 분배 기능부

111 : 인증처리 기능부 112 : 인증실패 처리 기능부

113 : 인증상태 관리 기능부 114 : 망인증 처리 기능부

115 : 인증상태 변경 기능부

116 : 인증관련처리 트래픽 수집 기능부

12 : 가입자 관리 시스템 접속부 13 : 등록처리부

14 : 키 관리부 15 : 보안정책/감사부

16 : 운용관리부　　17 : 서비스 관리부

18 : 시스템 관리부　　19 : 데이타베이스 시스템 관리 접속부

20 : 운용자 접속부　　21 : 데이타베이스 시스템 관리부

22 : 기능함수 저장부

발명의 상세한 설명

발명의 목적

발명이 속하는 기술 및 그 분야의 종래기술

본 발명은 인증처리 장치에서의 인증처리 방법에 관한 것으로, 이동통신 서비스를 제공할 경우, 서비스 불법 사용이나 단말기 복제 등으로 인한 사업자의 경제적 손실을 줄이고, 음성 및 신호를 암호화하여 가입자의 프라이버시를 보장하기 위해, 서비스 가입시에 가입자에게 인증키를 할당하고, 서비스 제공시에 할당된 인증키를 사용하여 인증을 수행하며, 이 인증 수행 결과를 이용하여 서비스 불법 사용 및 단말기 복제를 검출하고, 검출된 불법 사용으로부터의 해결책을 제시하는 기술에 관한 것이다.

현재 무선전화와 차량전화 서비스의 도입과 함께 이루어진 무선통신(이동통신) 서비스의 급속한 확장은 타 통신 서비스에 비해 괄목할 만한 성장을 보이고 있다. 그러나 무선전화와 차량전화는 그 자체가 가지고 있는 품질, 서비스 요금, 단말기 가격 등에서의 약점으로 인해 차세대 이동전화인 개인통신 서비스(PCS)로 수요전환이 예상되고 있다.

개인통신 서비스는 개인이 휴대용 단말장치를 이용하여 장소와 시간에 관계없이 개인간 음성 및 저속 데이터 통신을 할 수 있는 저렴한 가격의 보편적인 이동통신 서비스를 말한다.

이러한 개인통신 서비스로 가입자는 저렴하고 다양하며 편리한 서비스를 제공받을 수 있지만, 이로인해 새로운 문제점이 발생하였다.

즉, 무선이라는 특성을 이용한 서비스의 불법 이용 및 통화 도청이다.

서비스 불법 이용은 가입자에게는 부당한 과금 통지라는 문제를 초래하며, 사업자에게는 가입자와의 요금 분쟁으로 인한 이미지 실추 및 무선 자원 낭비라는 심각한 문제를 초래한다. 또한, 통화 도청은 가입자 입장에서의 프라이버시 침해가 된다.

이와 같은 문제를 해결하기 위해 기존 이동통신 사업자들은 여러가지 해결 방안을 모색하여 사용하고 있으나, 궁극적으로는 인증처리 장치 사용이 가장 바람직한 해결책으로 대두되고 있다.

이러한 인증처리 장치는 온라인으로 제시되는 인증 요구를 최대한 신속하게 처리하여 서비스에 미치는 영향을 최소화할 수 있을 정도의 성능을 가져야 하며, 가입자의 비밀키 및 인증 알고리즘이 외부에 노출되지 않도록 안전하게 보호하여 만일에 있을지도 모를 정보 유출로 인해 가입자에게 비밀키 재분배는 물론, 나아가서 단말기 교체라는 불편을 주지 않도록 구성되어야 한다.

그리고 상기와 같은 단순한 인증 기능 이외에도, 인증 처리로 인해 발생한 데이타를 감사하고, 불법 사용 및 불법 단말기

를 검출하며 이를 해결하는 기능을 제시해야 한다.

발명이 이루고자하는 기술적 과제

본 발명에서는 상기에 기술한 바와 같은 종래 요구사항을 감안하여, 인증처리 장치에서의 분배 기능, 인증처리 기능, 인증실패처리 기능, 인증상태 관리 기능, 망인증처리 기능, 인증상태 변경 기능 및 인증관련 처리 트래픽 수집 기능 등을 수행하기 위한 인증처리 방법을 제시하는 것을 목적으로 한다.

즉, 상기와 같은 기능을 통해 인증처리장치와 접속되는 타 장치와의 인터페이스를 규정하고 처리 흐름을 정의한다.

더욱 상세하게는 가입자 정보처리 시스템(이하 HLR이라 칭한다)으로 부터의 인증요구를 신속히 처리하기 위해 분배 기능을 두어 부하를 관리하도록 하고, 인증처리 장치가 요구하는 인증관련 작업은 망부하가 적은 시간에 요구하도록 한 것이다.

또한 인증처리 장치 내의 보안정책/관리부와의 신속한 정보교환을 위해 공유 메모리를 설정하여 보안정책/관리부가 제공하는 보안정책 결정에 따라 동작하도록 하고, 나머지 인증 결과 자료는 오프라인으로 로그에 기록하도록 하며, 운용관리 목적을 위해서는 인증 관련 작업 트래픽을 제공해주는 기능을 별도로 설정한 것이다.

발명의 구성 및 작용

상기와 같은 목적을 달성하기 위해 본 발명에서 제시한 인증처리 방법은, 인증처리 장치로 수신되는 모든 운답처리(TCAP) 프리미티브를 적당한 PCS 응용(PAP) 메시지로 변환시키고, 이를 해당하는 내부 기능으로 분배하는 분배 과정과;

인증을 요구한 단말기에 대한 비밀키 및 식별 정보를 사용하여 인증응답을 생성하고, 인증 성공/실패 여부를 판단하여 보안정책 결정을 확인하고 이를 요구하는 인증요구 처리 과정과;

단말기로 부터의 인증실패 보고를 받으면 보안정책/감사 수단과의 상호작용을 통하여 정한 작업을 수행하는 인증실패 처리 과정과;

인증 처리 기능, 인증실패처리 기능, 인증상태 변경 기능으로부터, 보안정책/감사부가 정한 정책 수행을 요청한 단말기의 작업 종료에 대한 처리를 위임받으면 이를 처리하는 인증상태관리 과정과;

임시 비밀키 변경시 단말기가 망을 인증하기 위한 요구를 보내면 이에 대한 인증응답을 생성하여 보내는 망 인증 과정과;

인증처리 장치 내부적인 과정에 의해 추가적인 인증 및 인증상태 변경이 필요하다고 판단되는 단말기에 대하여 인증을 요구하는 인증상태변경 과정과;

인증처리 장치와 송수신하는 인증관련 메시지의 트래픽을 측정하여 운용관리 목적으로 제공하는 인증관련처리트래픽 수집 과정을 포함하여 인증처리를 수행하는 것을 특징으로 한다.

상술한 목적 및 특징들, 장점은 첨부된 도면과 관련한 다음의 상세한 설명을 통하여 보다 분명해 질 것이다. 이하 첨부된 도면을 참조하여 본 발명의 실시예를 상세히 설명하면 다음과 같다.

도 1은 본 발명이 적용되는 개인통신서비스망의 기능을 블럭으로 나타낸 구성도로, 인증 서비스 제공 절차에 관한 처리 흐름을 나타낸다.

단말기(200)는 기본적인 호처리 및 위치등록 기능 이외에 인증 처리를 위해 가입자 비밀키(A-key)를 저장하고, 임시 비밀

키(Shared Secret Data : SSD), 신호 비화키(Signaling Message Encryption KEY : SMEKEY), 음성 비화키(CDMA Private Long Code Mask : CDMAPLCM)를 생성/저장하며, 또한 호 이력 카운트(Call History COUNT : COUNT)를 저장/갱신하고, 인증 및 비화 알고리즘 저장/수행등을 담당한다.

기지국/기지국 제어기(300)는 상기 단말기(200)와 교환기 사이에서 단말기(200)가 무선 프로트콜을 사용하여 망에 접근할 수 있도록 해주며, 보안과 관련하여는 비화 기능을 직접 수행한다.

교환기/방문자 정보처리 시스템(PCX/VLR)(400)은 인증을 위해 난수(RAND)를 생성하여 망내에 방송하는 기능을 수행한다.

가입자 정보처리 시스템(HLR)(500)은 인증을 위해 상기 교환기/방문자 정보처리 시스템(400)으로 부터의 인증관련 메시지를 인증처리 장치(100)로 중계하고, 또한, 인증처리 장치(100)로 부터의 인증관련 메시지를 위치추적하여 해당 교환기/방문자 정보처리 시스템(400)으로 중계하는 기능을 수행한다.

인증처리 장치(100)는 가입자 비밀키 및 임시 비밀키를 생성/저장하고 가입자에게 분배하며, 인증을 위한 난수(RAND)를 생성하며, 단말기(200)로 부터의 인증응답(AUTHR)을 확인하며, 신호비화키와 음성비화키를 생성/저장한다.

또한, 호 이력 카운트(COUNT)를 저장/갱신하며, 인증 및 비화 알고리즘을 저장하고 이를 수행한다. 온라인으로 처리되는 이러한 인증 관련 기능 이외에도,망내 인증 정책을 결정하고 이를 시행하며, 인증 관련 데이타를 감사하는 전체적인 보안 관리 기능도 수행한다.

가입관리 시스템(Customer Information System : CIS)(600)은 인증처리 장치와는 X.25로 연결되며, 신규 가입자 등록시 가입자 정보를 인증처리 장치로 전송하여 해당 가입자에게 비밀키가 할당되도록 해주며, 이후에 가입자가 인증 서비스를 받을 수 있도록 해준다.

도 2는 본 발명에 적용되는 개인통신망에서의 단말기 인증 절차를 나타낸 도면으로, 단말기(200)와 인증처리 장치(100)는 인증 절차가 수행되기 전인 가입 직후에 서로 동일한 가입자 인증용 비밀키(A-key)(a)를 보안상 안전한 방법을 통하여 분배하고 저장한 후;

임시 비밀키(SSD) 갱신 절차를 거쳐 서로 동일한 임시 비밀키도 저장한다;

이후, 단말기(200)가 망에 접속할 때는 망에서 보내온 난수(b)와 임시 비밀키, 그리고 기타 파라미터를 이용하여 인증응답(AUTHR)(c)을 생성하여 이를 인증처리 장치로 보낸다;

인증처리 장치(100)는 자신이 저장해 둔 해당 단말기 관련 정보를 이용하여 동일한 생성 과정을 거쳐 인증응답(d)을 계산하고 이를 단말기(200)가 보내 온 인증응답(c)과 동일한지 확인한다(e);

또한, 이때 단말기(200)가 보내 온 호 이력 카운트(COUNT)가 인증처리 장치(200)내의 카운트와 동일한지 확인한다(f);

상기와 같은 두 가지 비교 과정에서 단말기(200)와 인증처리 장치(100)의 계산 결과가 서로 같으면 인증에 성공한 것이고, 같지 않으면 인증에 실패한 것이 된다.

도 3은 본 발명이 적용되는 인증처리 장치의 내부 구성을 나타내는 블럭도로, 상기 가입자 정보처리 시스템(500)과의 접속을 위한 접속 장치로, 공통선 신호 채널을 통하여 가입자 정보처리 시스템(500)과 정보교환을 가능케하여 인증처리를 위해 필요한 메시지를 가입자 정보처리 시스템(500)과 송/수신할 수 있도록 하며, 또한, 공통선 신호로 송/수신되는 트래픽 및 공통선 신호의 상태를 측정하여 운용관리부(16)에 제공하고, 운용관리부(16)의 제어 요구에 의해 공통선 신호를 제어하는 기능을 수행하는 가입자 정보처리 시스템 접속부(10)와;

상기 가입자 정보처리 시스템 접속부(10)를 통해 수신된 인증 요구, 인증 상태보고, 인증실패보고, 기지국 시도 메시지를 처리하며, 인증처리 장치(100) 내부 결정에 의해 인증 상태 변경 절차를 수행하여 가입자 정보처리 시스템 접속부(10)를 통해 인증 상태 변경 메시지를 보내는 인증 요구 처리부(11)와;

상기 가입자 관리 시스템(600)에 접속하여 정보를 전송하며, 정보 송/수신 처리에 따른 트래픽 정보를 수집하는 가입자 관리 시스템 접속부(12)와;

인증 수행을 위해 필요한 가입자 정보를 관리하는 등록처리부(13)와;

인증 수행에 사용되는 가입자 비밀키(A-key)에 대한 관리를 수행하는 키 관리부(14)와;

인증 처리중에 얻어진 인증 처리 기록을 이용하여 단말기(200)의 보안 상태를 감사하고, 감사 자료로부터 각 인증 성공/실패에 대한 처리를 결정하는 보안정책/감사부(15)와;

인증처리 장치(100)의 하드웨어 및 인증 처리에 대한 운용관리를 수행하는 운용관리부(16)와;

상기 데이타베이스 시스템 관리부(21)에 구축된 모든 데이타베이스 테이블에서 각 데이타 필드들의 조합으로 이루어지는 통계 및 레코드들을 검색하여 운용자에게 제공하는 서비스 관리부(17)와;

응용 소프트웨어의 설치, 초기화, 기동 및 정지와 하드웨어 및 응용 소프트웨어의 형상 관리를 수행하고, 응용 소프트웨어에 대한 프로세스 관리 기능을 수행하는 시스템 관리부(18)와;

인증처리 장치(100)내의 데이타베이스인 가입자 데이타베이스와 운용관리 데이타베이스를 초기화하고 백업 및 복구하는 데이타베이스 시스템 관리 접속부(19)와;

운용자가 인증처리 장치(100) 내부 기능을 요구하고, 수행 결과를 화면으로 확인할 수 있는 환경을 제공하는 운용자 접속부(20)와;

가입자 데이타베이스(가입자 비밀키 포함)와 운용관리 데이타베이스로 구성되는 데이타베이스 시스템 관리부(21); 및

인증처리 장치(100)에 저장되어야 하는 인증 및 비화 관련 알고리즘의 집합체인 기능함수 저장부(22)를 포함하여 구성된다.

또한 상기 등록처리부(13)는 신규 가입자 등록 처리 및 기존 가입자 정보의 삭제, 변경 처리를 수행하고, 운용자 접속부(20)의 요구에 의해 기존 가입자에 대한 가입자 비밀키 재할당 기능을 수행하며, 등록된 가입자가 가입자 비밀키를 단말기(200)에 입력하도록 하는 가입자 비밀키 발송 절차도 수행한다.

키 관리부(14)는 가입자 비밀키를 생성하고 암호화하여 신규 가입자 등록 및 가입자 비밀키를 재할당시 이를 제공하고, 가입자 비밀키의 삭제, 검색, 폐기 처리를 수행한다. 또한 인증요구 처리부(11)에 가입자 비밀키를 제공하는 역할을 한다.

보안정책/감사부(15)는 특정 단말기의 불법이용 발생 가능성이 매우 높을 때는 적절한 조치를 취한 다음 운용자에게 경보를 보내고, 해당 단말기의 보안 관련 자료를 출력하기도 한다.

운용 관리부(16)는 가입자 정보처리 시스템 접속부(10), 인증 요구 처리부(11), 가입자 관리 시스템 접속부(12), 시스템 관리부(18), 데이타베이스 시스템 관리 접속부(19) 및 하드웨어 & 오퍼레이팅 시스템으로부터 트래픽 정보, 상태정보 등 측정정보를 정기적 또는 운용자의 요청에 의해 수집하고, 이를 분석하여 데이타베이스 시스템 관리부(21)에 저장한다.

또한, 운용자의 요구에 의한 운용관리 파라미터 설정 및 시스템 신호(No.7) 제어등을 위한 기능을 가진다. 아울러 실시간 출력이 필요한 정보는 운용자 접속부(20)로 전달하여 운용자가 운용관리 정보를 실시간으로 알 수 있게 한다.

서비스 관리부(17)는 운용관리부(20)를 통해 데이타베이스 시스템 관리부(21)에 저장된 각종 측정 정보(트래픽, 상태 등)에 대한 통계처리 및 운용정보 검색(이력, 상세) 기능을 운용자에게 제공할 수 있도록 한다.

데이타베이스 시스템 관리 접속부(19)는 데이타베이스 초기화시에는 시스템 관리부(18)의 요구에 의하여 수행하며, 나머

지 기능은 운용자가 작업석에서 입력하는 명령어에 의해 수행된다.

또한, 운용관리 기능 장애시 운용자가 직접 데이타베이스에 접속하여 운용할 수 있는 기능도 제공하며, 데이타베이스 시스템 관리부(21)가 제공하는 상태정보를 수집하여 운용관리부(16)의 요구가 있을때 제공하기도 한다.

운용자 접속부(20)는 운용자가 화면형태로 입력하는 명령어 수행 요구는 물론, 명령어 형태의 수행 요구도 처리하며 명령어 화일로 여러 개의 명령어를 한번에 수행할 수 있는 기능도 제공한다.

명령어 입력시에는 명령어 자체에 대한 문법/의미 분석을 거쳐서 해당 기능 블럭에 명령어 수행을 요구한다.

또한 운용자가 시스템에 로그인할 수 있는 기능을 제공하며, 운용자 관련 계정을 추가/삭제/검색/변경할 수 있는 기능도 제공하며, 운용자가 명령어 수행시에, 수행한 명령어를 시스템 접근 이력 파일에 추가하여 운용자가 원하는 경우에 시스템에 접근한 이력을 제공한다.

그리고 명령어 수행 요구시 도움말도 제공한다.

마지막으로 기능함수 저장부(21)내의 라이브러리 구성요소를 보면, 이는 가입자 비밀키 보안을 위한 암호/복호 알고리즘, 인증응답 생성 알고리즘, 임시 비밀키 생성 알고리즘, 신호비화키 생성 알고리즘, 음성비화키 생성 알고리즘이며, 각 알고리즘 필요시 인증요구 처리부(11)가 사용한다.

도 4는 본 발명이 적용되는 상기 인증요구 처리부(11)의 내부 상세 구성도로, 인증처리 장치(100)로 수신되는 모든 문답처리(TCAP) 프리미티브를 받아서 이를 적당한 PCS 응용(PCS Application Part : 이하 PAP라 칭한다) 메시지로 바꾸어 처리하는 분배 기능부(110)와;

상기 분배 기능부(110)로 부터 수신된 인증요구를 처리하는 부로, 인증 알고리즘을 통해 인증 결과값을 생성하여 인증 성공/실패 여부를 판단한 후, 해당 특정 가입자 식별 번호(Mobile Identification Number : MIN)에 대한 인증센터의 보안관리 정책이 결정된 경우 이를 수행하기 위한 데이타를 발생시키고, 이어 발생 데이타를 인증 응답과 함께 단말기에 보낸 다음, 인증상태 관리 기능부(113)로 후속 작업 수행을 요구하는 인증 처리 기능부(111)와;

상기 분배 기능부(110)로 부터 수신된 인증실패 보고를 처리하는 기능부로, 인증실패 보고를 이용하여 보고된 유형에 따라 상기 보안정책/감사부(15)로 내역을 보고한 후 그에 대한 정책 결정 결과를 받아 후속 작업을 수행하는 인증실패 처리 기능부(112)와;

상기 분배 기능부(110)로부터 수신된 인증상태 보고를 처리하는 인증상태 관리 기능부(113)와;

상기 분배 기능부(110)로 부터 수신된 망인증 요구를 처리하는 부로, 망인증 요구에 저장된 기지국 시도용 난수(RANDBS)를 이용하여 인증 알고리즘을 수행한 후, 결과값인 기지국 인증응답(AUTHBS)을 포함한 망인증요구 응답을 분배 기능부(110)로 출력하는 망인증 처리 기능부(114)와;

상기 보안정책/감사부(15)로 부터의 인증상태 변경 요구를 처리하는 인증상태 변경 기능부(115); 및

인증관련처리 트래픽 수집 기능부(116)를 포함하여 구성된다.

또한, 상기 분배 기능부(110)는 인증처리 장치(100)로 수신되는 메시지의 오류를 검사하고, 인증처리 관련 응용 프로세스 사이의 부하도 조절하면서 수신된 TCAP 프리미티브에 해당하는 응용 프로세스로 PAP 메시지를 보내며, 인증상태 변경 요구가 있는 경우 해당하는 TCAP 프리미티브를 가입자 정보처리 시스템 접속부(10)로 출력한다.

인증실패 처리 기능부(113)에서는 상기 후속 작업 수행시 이를 위해 인증 알고리즘을 이용하여 해당하는 데이타를 발생시킨 후 인증실패 보고 응답을 이용하여 분배 기능부(110)로 출력한 다음, 인증상태 관리 기능부(113)로 인증상태 관리를 요청한다.

인증상태 관리 기능부(113)는 상기 보안정책/감사부(15)의 정책 결정에 의해 인증처리 기능부(111), 인증실패 처리 기능부(112), 인증상태 변경 기능부(115)에서 특정 가입자 식별 번호, 장치 일련 번호(Equipment Serial Number : ESN)에 대하여 수행한 작업에 대한 결과를 보고받고, 이 보고된 결과의 성공/실패 여부를 판단하여 보안정책/감사부에 보고한 후 후속 작업이 더 필요한 경우에 보안정책/감사부의 정책 결정에 따라 후속 작업을 수행한다.

인증 상태 변경 기능부(115)는 특정 가입자의 인증상태 변경 요구를 받으면 해당하는 특정 가입자 식별 번호와, 장치 일련 번호의 인증상태 변경을 처리하기 위해 인증 알고리즘을 이용하여 보안 정책/감사부(15)가 원하는 작업에 해당하는 데이타를 발생시킨 후, 인증상태 변경 요구를 가입자 정보처리 시스템 접속부(10)로 출력한다.

그리고 인증 요구 처리부(11)가 수행하는 메시지들의 성공/실패 여부와 처리 내역을 수집하여 운용관리부(16)가 원하는 경우 이를 제공하는 기능을 수행한다.

이와 같은 인증요구 처리 장치는 상기에서 언급된 바와 같이, 단말기로 부터의 인증요구를 온라인으로 처리해야 하는 장치이므로, 접속되어 있는 다른 장치들과의 연관관계가 얼마나 긴밀한가가 중요하다.

또한, 단순히 비밀키로부터 인증응답을 만드는 인증요구 처리 뿐만 아니라 정기 또는 비정기적인 유일시도 요구, 공유비밀데이타(SSD) 갱신등을 단말기에게 요구하고, 처리 결과를 모니터링해야 하며, 이 모든 처리 결과를 로그에 저장하여 보안정책/감사부가 온라인 및 오프라인으로 감사하여 불법 사용 및 복제가 의심되는 가입자에 대한 별도의 조치가 이루어져야 한다.

그리고 인증요구 처리 장치 및 보안정책/감사부 간의 신속한 정보교환을 위해 효율적인 두 장치간 인터페이스가 정의되어야 한다.

상기와 같이 구성된 인증처리 장치의 동작을 개략적으로 설명하면, 가입자가 새로 등록할 단말기(200)에 대한 정보를 가입자 관리 시스템(600)에 입력하여 가입신청을 하면, 가입자 관리 시스템(600)에서는 상기 정보 중 인증에 필요로되는 정보를 인증처리 장치(100)로 전송한다.

인증처리 장치(100)에서는 신규 가입자의 추가를 담당하는 등록처리부(13)와, 상기 신규 가입자에게 부여할 가입자 비밀키를 생성하여 할당하는 키 관리부(14)를 통해 키를 분배받는다.

이는 상기 가입자 관리 시스템(600)을 통해 단말기(200)로 전송된다.

이처럼 키가 주입되면 단말기(200)에서는 인증처리 장치(100) 간 동일한 가입자 인증용 비밀키와, 임시 비밀키 갱신 절차를 통해 생성된 동일한 임시 비밀키를 저장하고 있는 상태에서 통신을 시도하게 되는 바, 파워-키를 작동시킴과 동시에 단말기(200)가 망에서 보내온 난수와 임시 비밀키 그리고 기타 파라미터를 이용하여 인증응답을 생성해 이를 인증처리 장치(100)로 보낸다.

인증처리 장치(100)에서는 인증요구처리부(11)를 통해 상기 단말기(200)의 인증을 수행하고 이의 결과를 가입자 정보처리 시스템(500)으로 전송한다.

가입자 정보처리 시스템(500)에서는 상기 인증관련 메시지를 위치추적하여 해당 교환기/방문자 정보처리 시스템(400)으로 전송하여 현재의 단말기(200)가 등록이 된 상태임을 알린다.

이에 따라 현 단말기(200)의 위치가 교환기에 등록되고, 가입자가 전송하는 전화번호에 따라 상대방과의 통화가 시작된다.

그리고 인증처리 장치의 보안정책/감사부(15)와 서비스 관리부(17) 및 운용관리부(16) 등을 통해 운용자는 단말기(200)의 보안 상태 및 각 가입자에 대한 정보 등을 관리할 수 있다.

이하, 상기 인증요구 처리부(11)의 기능상 처리 과정을 각 순서도를 참조하여 설명하면 하기와 같다.

도 5는 상기 인증요구 처리부(11) 내의 분배 기능부(110)에 적용되는 분배 기능의 처리 과정을 나타낸 순서도로, 분배 기능은 항상 대기 상태로 존재한다(A1).

이와 같은 대기 상태에서 HLR로 부터 문답처리(이하 TCAP라 칭한다) 프리미티브를 수신하거나, 인증상태 변경 기능으로부터 인증상태 변경 요구가 수신될 경우(A2) 동작한다.

이때 HLR로 부터 TCAP 프리미티브가 수신된 경우, 수신된 TCAP 프리미티브의 종류를 판단하며, 판단 결과 인증 요구인 경우(A3), 인증처리 기능에 처리를 요청한 후, 대기상태에 있다가(A31) 응답이 수신되면 이에 대한 결과 TCAP 프리미티브를 HLR로 송신한다(A32).

상기 판단결과 인증상태 보고인 경우(A4)에는, 인증상태 보고 처리 기능에 처리를 요청한 후, 대기상태에 있다가(A41) 응답이 수신되면 이에 대한 결과 TCAP 프리미티브를 HLR로 송신한다(A42).

상기 판단결과 인증실패보고인 경우(A5)에는, 인증실패보고 처리 기능에 처리를 요청한 후, 대기상태에 있다가(A51) 응답이 수신되면 이에 대한 결과 TCAP 프리미티브를 HLR로 송신한다(A52).

상기 판단 결과 망인증 요구인 경우(A6)에는, 망 인증처리 기능에 처리를 요청한 후, 대기상태에 있다가(A61) 응답이 수신되면 이에 대한 결과 TCAP 프리미티브를 HLR로 송신한다(A62).

상기 판단 결과 마지막으로 상기 모든 경우에 속하지 않는 TCAP 프리미티브는 이전에 HLR로 송신한 인증상태변경 요구에 대한 응답으로 인지하고, 이를 인증상태변경 기능으로 보낸다(A7).

그리고 상기 모든 경우(A3 ~ A7) 중 선택되어 수행된 경우에서 마지막에 송신된 TCAP 프리미티브는 인증관련 처리 트래픽 수집 기능부에 수신되며, 상기 프리미티브를 수신한 트래픽 수집 기능부에서는 운용관리를 위해 HLR과의 트래픽 정보를 저장한 후 대기 상태로 전환된다(A8).

한편, 대기 상태에서 인증상태변경 기능으로부터의 요구가 있으면(A2), HLR과의 통신부하를 측정하여(A9) 과부하 상태이면 과부하 상태가 아닐때까지 기다린 후, HLR로 TCAP 프리미티브를 송신한 다음 대기 상태로 전환한다(A9).

도 6은 상기 인증요구 처리부(11) 내의 인증 처리 기능부(111)에 적용되는 인증 처리 기능의 처리 과정을 나타낸 순서도로, HLR로 부터 인증 요구가 수신되면, 인증 대상 가입자의 식별자인 MIN과 장치식별자인 ESN이 인증처리 장치에 등록된 가입자의 것인지 검사한 후, 등록되지 않은 경우이면 인증 실패로 간주하고 종료한다(B1).

검사 결과 MIN, ESN이 합법적인 가입자의 것이면, 시스팀 접근 유형이 플래시 요구인지 검사한다(B2).

검사 결과 플래시 요구이면 유일시도를 수행해야 하므로, 난수(RANDU)를 입력하여 인증알고리즘(이하 케이브(CAVE)라고 칭한다)을 수행해 결과값인 인증응답(AUTHU)를 얻은 후, 단말기 상태를 유일시도중으로 세팅한다(B21),

이어 상기 인증 결과를 HLR로 송신한 다음, 해당 가입자에 대한 인증상태 관리 요청을 한 후 종료한다(B22).

검사 결과 플래시 요구가 아닌 나머지 시스팀 접근 유형에 대하여는 일단 단말기가 사용한 난수와 동일한 난수를 입력으로 케이브를 수행하여 결과값인 인증응답을 얻은 후(B23), 상기 인증응답과 단말기가 보낸 인증응답이 상호 동일한지 여부를 판단한다(B24).

그리고 인증처리 장치가 저장하고 있던 카운트(COUNT) 값도 단말기가 보낸 카운트 값과 동일한지 판단한다(B24).

이때 상기 두개 판단 결과 둘 중에 하나만 일치하지 않아도 인증 실패로 보고, 보안정책/감사부에 결과를 보고한 다음, 이어서 정해진 정책을 수신한다(B25).

한편, 상기 두개 판단 결과 인증응답과 카운트 모두 일치하는 경우에는 시스팀 접근 유형이 호 발신 또는 호 착신인지 검

사하여, 둘 중 하나인 경우에는 다시 케이브를 수행하여 음성 비화키(COMAPLCM)와 신호메시지 비화키(SMEKEY)를 생성한다(826).

인증 성공은 물론 인증 실패시에도 보안정책/감사 장치가 정해놓은 정책을 확인하여 시도해야한다.

이어 보안정책/감사부가 정한 정책이 임시 비밀키(SSD) 갱신이면(B3) 난수형태의 임시 비밀키(RANDSSD)를 입력으로 케이브를 수행하여 결과값인 임시 비밀키를 만들고 단말기 상태를 임시 비밀키 갱신중으로 세팅한다(831).

또한, 임시 비밀키 갱신시에는 유일시도를 연달아 수행하므로 난수를 입력으로 케이브를 수행하여 결과값 인증응답을 생성한 후, 단말기 상태를 유일시도중으로 세팅한다(832).

한편, 보안정책/감사부가 정한 정책이 유일시도 요구이면(B4) 난수를 입력으로 케이브를 수행하여 결과값인 인증응답을 생성한 후, 단말기 상태를 유일시도중으로 세팅한다(841).

그리고 상기 임시 비밀키 갱신(B3) 또는 유일시도 처리(B4)후 에는 보안정책/감사부가 정한 정책에 카운트 변경이 있는지 검사하여 요구하는 경우(B5), 카운트 증가에 필요한 작업을 수행하고 단말기 상태를 카운트 갱신중으로 세팅한다(851).

그런다음 인증 결과를 HLR로 송신한 후, 단말기 상태가 세팅되어 있으면 인증상태 관리를 요청한 다음 종료하고, 그렇지 않으면 곧바로 종료한다(852).

도 7은 상기 인증요구 처리부(11) 내의 인증 실패 처리 기능부(112)에 적용되는 인증 실패 처리 기능의 처리 과정을 나타낸 순서도로, HLR로부터 인증실패처리 요구를 수신하면 요구가 인증실패 목적인지 인증처리 장치(AC)가 지시한 작업에 대한 보고 목적인지를 판단하여, 순수한 인증실패인 경우에는 보안정책/감사부에 보고하고 결정에 따른다(C1).

인증처리 장치가 지시한 작업에 대한 보고인 경우에는 보고 목적이 임시 비밀키 갱신 성공이면 단말기에서 사용하는 임시 비밀키가 새로운 임시 비밀키 이므로 인증처리 장치에서 사용하는 임시 비밀키도 새로운 임시 비밀키로 변경한다(C2).

반대로 임시 비밀키 변경 실패이면 보안정책/감사부에 보고하고 결정에 따른다(C3).

또한, 보고 목적이 카운트 변경 성공이면 인증처리 장치 내의 해당 가입자 카운트를 증가시키고(C4), 카운트 변경 실패이면 보안정책/감사부에 보고하고 결정에 따른다(C5).

또한, 보고 목적이 유일시도 성공이면 보안정책/감사부가 정해놓은 정책을 확인하고, 유일시도 실패이면 보안정책/감사부에 보고하고 결정에 따른다(C6).

이때 상기에서 보안정책/감사부가 정한 정책이 임시 비밀키 갱신(C7)이면 난수형태의 임시 비밀키(RANDSSD)를 입력으로 케이브를 수행하여 결과값인 임시 비밀키를 만들고, 단말기 상태를 임시 비밀키 갱신중으로 세팅한다(C71).

또한, 임시 비밀키 갱신시에는 유일시도를 연달아 수행하므로 난수를 입력으로 케이브를 수행하여 결과값 인증응답을 생성한 후, 단말기 상태를 유일시도중으로 세팅한다(C72).

그리고 보안정책/감사부가 정한 정책이 유일시도 요구이면(C8), 난수를 입력으로 케이브를 수행하여 결과값 인증응답을 생성한 후, 단말기 상태를 유일시도중으로 세팅한다(C81).

그리고 상기 임시 비밀키 갱신(C7) 또는 유일시도 처리(C8)후 에는 보안정책/감사부가 정한 정책에 카운트 변경이 있는지 검사하여 요구하는 경우(C9), 카운트 증가에 필요한 작업을 수행하고 단말기 상태를 카운트 갱신중으로 세팅한다(C91).

그런다음 인증 실패 보고에 대한 응답을 HLR로 송신한 후, 단말기 상태가 세팅되어 있으면 인증상태 관리를 요청한 다음 종료하고, 그렇지 않으면 곧바로 종료한다(C92).

도 8은 상기 인증요구 처리부(11) 내의 인증 상태 관리 기능부(113)에 적용되는 인증 상태 관리 기능의 처리 과정을 나타

낸 순서도로, 인증처리 기능, 인증실패처리 기능 및 인증상태 변경 기능으로 부터 인증상태 관리 요구가 수신되면(01), 해당 가입자에 대한 타이머를 설정(

Ⓐ)하고 HLR로부터 인증상태보고를 수신할때까지 기다린다(02).

타이머가 끝날때까지 수신되지 않으면(03), 단말기 상태를 확인하여 단말기 상태가 임시 비밀키 갱신중이면 새로운 임시 비밀키로 사용할 계획이던 임시 비밀키를 삭제하고, 이어 단말기 상태를 리셋한 후 보안정책/감사부에 보고한 다음 결정에 따른다(031).

상기 판단 결과 단말기 상태가 임시 비밀키 갱신중이 아니면 나머지 단말기 상태를 모두 리셋하고 보안정책/감사부에 보고한 후 결정에 따른다.(032)

한편, HLR로 부터 인증상태보고가 수신되면 단말기 상태를 모두 리셋하고 보고 목적에 따라 작업을 수행한다(04).

이때 보고 목적이 임시 비밀키 변경 성공이면 현재 임시 비밀키를 새로운 임시 비밀키로 변경하고, 임시 비밀키 변경 실패이면 보안정책/감사부에 보고한 후 결정에 따른다(05).

또한, 보고 목적이 카운트 변경 성공이면 인증장치 내의 해당 가입자 카운트를 증가시키고, 카운트 변경 실패이면 보안정책/감사부에 보고하고 결정에 따른다(06).

또한, 보고 목적이 유일시도 성공이면 보안정책/감사부가 정해놓은 정책을 확인한다. 그리고 유일시도 실패이면 보안정책/감사부에 보고하고 결정에 따른다(07).

이어 보안정책/감사부가 정한 정책이 임시 비밀키(SSD) 갱신이면(08) 난수형태의 임시 비밀키(RANDSSD)를 입력으로 케이브를 수행하여 결과값인 임시 비밀키를 만들고 단말기 상태를 임시 비밀키 갱신중으로 세팅한다(081).

또한, 임시 비밀키 갱신시에는 유일시도를 연달아 수행하므로 난수를 입력으로 케이브를 수행하여 결과값 인증응답을 생성한 후, 단말기 상태를 유일시도중으로 세팅한다(082).

한편, 보안정책/감사부가 정한 정책이 유일시도 요구이면(09) 난수를 입력으로 케이브를 수행하여 결과값인 인증응답을 생성한 후, 단말기 상태를 유일시도중으로 세팅한다(091).

그리고 상기 임시 비밀키 갱신(08) 또는 유일시도 처리(09)후 에는 보안정책/감사부가 정한 정책에 카운트 변경이 있는지 검사하여 요구하는 경우(010), 카운트 증가에 필요한 작업을 수행하고 단말기 상태를 카운트 갱신중으로 세팅한다(011).

그런다음 인증실패 보고에 대한 응답을 HLR로 송신한 후, 단말기 상태가 세팅되어 있으면 다시 타이머를 설정(

Ⓐ)하고 대기 상태로 전환한다(012).

도 9는 상기 인증요구 처리부(11) 내의 망인증 처리 기능부(114)에 적용되는 망인증 처리 기능의 처리 과정을 나타낸 순서도로, 분배기능으로 부터 망인증 요구가 수신되면(E1) 기지국 시도용 난수(RANDBS)를 입력으로 케이브를 수행한 후, 결과값인 기지국 인증응답(AUTHBS)을 생성한다(E2). 그런다음 상기 생성된 기지국 응답을 송신한 후 종료한다(E3).

도 10은 상기 인증요구 처리부(11) 내의 인증상태 변경 기능부(115)에 적용되는 인증상태변경 처리 과정을 나타낸 순서도로, 보안정책/감사부가 인증상태변경 결정을 내려 인증상태변경 기능이 요구되면 보안정책/감사부의 결정이 무엇인지를 판단한다. 판단 결과 보안정책/감사부가 정한 정책이 임시 비밀키 갱신이면(F1) 난수용 임시 비밀키(RANDSSD)를 입력으로 케이브를 수행하여 결과값인 임시 비밀키를 만들고, 이어 단말기 상태를 임시 비밀키 갱신중으로 세팅한다(F11).

또한, 임시 비밀키 갱신시에는 유일시도를 연달아 수행하므로 난수를 입력으로 케이브를 수행하여 결과값 인증응답을 생성한 후, 단말기 상태를 유일시도중으로 세팅한다(F12).

한편, 보안정책/감사부가 정한 정책이 유일시도 요구이면(F2) 난수를 입력으로 케이브를 수행하여 결과값 인증응답을 생성한 후, 단말기 상태를 유일시도중으로 세팅한다(F21).

그리고 상기 임시 비밀키 갱신(F1) 또는 유일시도 처리(F2)후 에는 보안정책/감사부가 정한 정책에 카운트 변경이 있는지 검사하여 요구하는 경우(F3), 카운트 증가에 필요한 작업을 수행하고 단말기 상태를 카운트 갱신중으로 세팅한다(F31).

그런다음 인증상태변경 요구를 HLR로 송신한 후 결과를 기다린다(F32).

인증상태변경 결과가 HLR로 부터 수신되면(F4) 실패 및 성공 여부를 판단하여(F41) 성공인 경우는 단말기 상태가 세팅되어 있는지 검사하여, '임시 비밀키 갱신중', '유일시도중', '카운트 갱신중' 중 하나라도 세팅되어 있으면 인증상태 관리를 요구하고 종료한다(F42).

상기 판단(F41) 결과 실패인 경우는 단말기 상태가 '임시 비밀키 갱신중'인 경우에만 새로 발생시켜 놓았던 임시 비밀키를 삭제하고(F43) 나머지 경우에는 단말기 상태만 리셋한 후 인증처리 장치 내에서 가입자의 인증상태를 변경전 상태로 만들어 놓기 위한 처리를 수행한 후 종료한다(F44).

도 11은 상기 인증요구 처리부(11) 내의 인증관련 처리 트래픽 수집 기능부(116)에 적용되는 인증관련처리트래픽 수집 기능의 처리 과정을 나타낸 순서도로, 본 기능은 항상 대기 상태로 관련 트래픽을 수집한다(G1).

내부 기능들로부터 인증관련 처리 트래픽 정보가 수신되면 관리하고 있던 해당 트래픽 항목을 증가시킨 후 종료한다(G2).

그리고 운용관리부로 부터 관리하던 트래픽 정보 요구가 수신되면 해당 항목의 현재값을 운용관리 장치로 송신하고, 관리하던 항목값은 리셋한다(G3).

이와 같이 본 발명은 현재 급부상하고 있는 개인통신 서비스에서 발생할 수 있는 서비스의 불법사용 및 통화 도청의 문제를 방지하는 인증처리 장치 내에서 인증요구에 적용되는 방법을 제공하여 효율적인 인증처리가 이루어지도록 한다.

발명의 효과

이상에서 상세히 설명한 바와 같이 이통통신에 관련되는 모든 통신 서비스에 본 발명을 사용하게 되면, 불법 가입자 및 불법 단말기를 검출하므로써 사업자의 경제적 손실을 차단하는 잇점이 있고, 불법 도청을 방지하므로써 가입자의 프라이버시 보호 잇점이 있으며, 보안정책 감사 기능을 통하여 다양한 형태의 보안 관리를 총괄적으로 수행할 수 있는 장점이 있다.

또한 인증 수행으로 인해 망 부하에 주는 영향을 최소화 할 수 있는 잇점이 있고, 인증요구 처리 장치를 보안정책 및 감사 장치와 분리시키므로써, 사업자가 원하는 보안정책 및 감사장치로의 변경이 용이한 잇점을 수반한다.

아울러 본 발명의 바람직한 실시예는 예시의 목적을 위해 개시된 것이며, 당업자라면 본 발명의 사상과 범위안에서 다양한 수정, 변경, 부가등이 가능할 것이며, 이러한 수정 변경 등은 이하의 특허 청구의 범위에 속하는 것으로 보아야 할 것이다.

(57) 청구의 범위

청구항 1. 인증처리 장치로 수신되는 모든 운답처리(TCAP) 프리미티브를 적당한 PCS 응용(PAP) 메시지로 변환시키고, 이를 해당하는 내부 기능으로 분배하는 분배 과정과;

인증을 요구한 단말기에 대한 비밀키 및 식별 정보를 사용하여 인증응답을 생성하고, 인증 성공/실패 여부를 판단하며 보

안정책 결정을 확인하고 이를 요구하는 인증요구 처리 과정과;

단말기로 부터의 인증실패 보고를 받으면 보안정책/감사 수단과의 상호작용을 통하여 정한 작업을 수행하는 인증실패 처리 과정과;

인증 처리 기능, 인증실패처리 기능, 인증상태 변경 기능으로부터, 보안정책/감사부가 정한 정책 수행을 요청한 단말기의 작업 종료에 대한 처리를 위임받으면 이를 처리하는 인증상태관리 과정과;

임시 비밀키 변경시 단말기가 망을 인증하기 위한 요구를 보내면 이에 대한 인증응답을 생성하여 보내는 망 인증 과정과;

인증처리 장치 내부적인 과정에 의해 추가적인 인증 및 인증상태 변경이 필요하다고 판단되는 단말기에 대하여 인증을 요구하는 인증상태변경 과정과;

인증처리 장치와 송수신하는 인증관련 메시지의 트래픽을 측정하여 운용관리 목적으로 제공하는 인증관련처리트래픽 수집 과정을 포함하여 인증처리를 수행하는 것을 특징으로 하는 인증처리 장치에서의 인증처리 방법.

청구항 2. 청구항 1에 있어서,

상기 분배 과정은, 대기 상태중에서 가입자 정보처리 시스템(HLR)으로 부터 TCAP 프리미티브가 수신된 경우, 수신된 TCAP 프리미티브의 종류를 판단한 후, 이 판단결과에 따라 그에 해당하는 작업을 수행할 수 있도록 각 기능 처리 수단에 처리를 요청하는 과정과;

상기 해당되는 작업을 수행한 후 생성된 결과인 TCAP 프리미티브를 인증관련 처리 트래픽 수집 기능부에 송신하는 과정과;

상기 프리미티브를 수신한 트래픽 수집 기능부에서는 운용관리를 위해 HLR과의 트래픽 정보를 저장한 후 대기 상태로 전환하는 과정; 및

상기 대기 상태중에서 인증상태변경 기능으로부터의 요구가 있으면, HLR과의 통신부하를 측정하여 과부하 상태이면 과부하 상태가 아닐때까지 기다린 후, HLR로 TCAP 프리미티브를 송신한 다음 대기 상태로 전환하는 과정을 포함하여 인증처리를 수행하는 것을 특징으로 하는 인증처리 장치에서의 인증처리 방법.

청구항 3. 청구항 1에 있어서,

상기 수신된 TCAP 프리미티브의 종류를 판단 결과 인증 요구인 경우 인증처리 기능에 처리를 요청하고, 인증상태 보고인 경우에는 인증상태 보고 처리 기능에 처리를 요청하고, 인증실패보고인 경우에는 인증실패보고 처리 기능에 처리를 요청하고, 망인증 요구인 경우에는 망 인증처리 기능에 처리를 요청한 다음;

상기 각 요청후에 대기상태에 있다가 응답이 수신되면 이에 대한 결과 TCAP 프리미티브를 HLR로 송신하는 과정과;

상기 수신된 TCAP 프리미티브의 종류 판단 결과 상기 모든 경우에 속하지 않는 TCAP 프리미티브는 이전에 HLR로 송신한 인증상태변경 요구에 대한 응답으로 인지하고, 이를 인증상태변경 기능으로 전송하는 과정을 포함하여 인증처리를 수행하는 것을 특징으로 하는 인증처리 장치에서의 인증처리 방법.

청구항 4. 청구항 1에 있어서,

상기 인증요구 처리 과정은, HLR로 부터 인증 요구가 수신되면, 인증 대상 가입자 식별자(MIN)와 장치 식별자(ESN)가 인증처리 장치에 등록된 가입자의 것인지 검사한 후, 등록되지 않은 경우이면 인증 실패로 간주하고 종료하는 과정과;

검사 결과 MIN, ESN이 합법적인 가입자의 것이면, 시스템 접근 유형이 플래시 요구인지 검사하는 과정과;

검사 결과 플래시 요구이면 유일시도를 수행해야 하므로, 난수를 입력하여 인증알고리즘(CAVE)을 수행해 결과값인 인증응답를 얻은 후, 단말기 상태를 유일시도중으로 세팅하는 과정과;

이어 상기 인증 결과를 HLR로 승신한 다음, 해당 가입자에 대한 인증상태 관리 요청을 한 후 종료하는 과정을 포함하여 인증처리를 수행하는 것을 특징으로 하는 인증처리 장치에서의 인증처리 방법.

청구항 5. 청구항 4에 있어서,

상기 검사 결과 플래시 요구가 아닌 나머지 시스템 접근 유형에 대하여는 일단 단말기가 사용한 난수와 동일한 난수를 입력으로 케이브를 수행하여 결과값인 인증응답을 얻은 후, 상기 인증응답과 단말기가 보낸 인증응답이 상호 동일한지 여부를 판단하는 과정과;

이어 인증처리 장치가 저장하고 있던 카운트도 단말기가 보낸 카운트와 동일한지 판단하는 과정과;

상기 두 판단 결과 둘 중에 하나만 일치하지 않아도 인증 실패로 인지하고서, 보안정책/감사부에 결과를 보고한 다음, 정해진 정책을 따르는 과정을 포함하여 인증처리를 수행하는 것을 특징으로 하는 인증처리 장치에서의 인증처리 방법.

청구항 6. 청구항 5에 있어서,

상기 두 판단 결과 인증응답과 카운트 모두 일치하는 경우에는 시스템 접근 유형이 호 발신 또는 호 착신인지 검사하여, 둘 중 하나인 경우에는 다시 케이브를 수행하여 음성 비화키와 신호메시지 비화키를 생성하는 과정을 포함하여 인증처리를 수행하는 것을 특징으로 하는 인증처리 장치에서의 인증처리 방법.

청구항 7. 청구항 5에 있어서,

상기 보안정책/감사부에서 정한 정책이 임시 비밀키 갱신에 관한 처리이면, 난수형태의 임시 비밀키를 입력으로 케이브를 수행하여 결과값인 임시 비밀키를 만들고 단말기 상태를 임시 비밀키 갱신중으로 세팅하는 과정과;

임시 비밀키 갱신시 유일시도의 연달은 수행을 위해 난수를 입력으로 케이브를 수행하여 결과값 인증응답을 생성한 후, 단말기 상태를 유일시도중으로 세팅하는 과정과;

상기 과정 후 보안정책/감사부에서 정한 정책에 카운트 변경이 있는지 여부를 판별하여 이에 해당하는 처리를 하는 과정을 포함하여 인증처리를 수행하는 것을 특징으로 하는 인증처리 장치에서의 인증처리 방법.

청구항 8. 청구항 5에 있어서,

상기 보안정책/감사부에서 정한 정책이 유일시도 요구이면, 난수를 입력으로 케이브를 수행하여 결과값인 인증응답을 생성한 후, 단말기 상태를 유일시도중으로 세팅하는 과정과;

상기 과정 후 보안정책/감사부에서 정한 정책에 카운트 변경이 있는지 여부를 판별하여 이에 해당하는 처리를 하는 과정을 포함하여 인증처리를 수행하는 것을 특징으로 하는 인증처리 장치에서의 인증처리 방법.

청구항 9. 청구항 7 또는 청구항 8에 있어서,

보안정책/감사부에서 정한 정책에 카운트 변경 요구가 있으면, 카운트 증가에 필요한 작업을 수행하고 단말기 상태를 카운트 갱신중으로 세팅하는 과정과;

상기 과정 후 발생된 인증 결과를 HLR로 송신한 후, 단말기 상태가 세팅되어 있는지 판별하는 과정과;

판별 결과 세팅되어 있으면 인증상태 관리를 요청한 다음 종료하고, 그렇지 않으면 곧바로 종료하는 과정을 포함하여 인증처리를 수행하는 것을 특징으로 하는 인증처리 장치에서의 인증처리 방법.

청구항 10. 청구항 1에 있어서,

상기 인증실패 처리 과정은, HLR로 부터 인증실패처리 요구를 수신하면 요구가 인증실패 목적인지 인증처리 장치가 지시한 작업에 대한 보고 목적인지를 판단하여, 순수한 인증실패인 경우에는 보안정책/감사부에 보고하고 결정에 따르는 과정과;

상기 판단결과 인증처리 장치가 지시한 작업에 대한 보고인 경우에는, 보고 목적이 임시 비밀키 갱신 성공이면 단말기에서 사용하는 임시 비밀키가 새로운 임시 비밀키 이므로 인증처리 장치에서 사용하는 임시 비밀키도 새로운 임시 비밀키로 변경하는 과정과;

임시 비밀키 변경 실패이면 보안정책/감사부에 보고하고 결정에 따르는 과정과;

보고 목적이 카운트 변경 성공이면 인증처리 장치 내의 해당 가입자 카운트를 증가시키고, 카운트 변경 실패이면 보안정책/감사부에 보고하고 결정에 따르는 과정; 및

보고 목적이 유일시도 성공이면 보안정책/감사부가 정해놓은 정책을 확인하고, 유일시도 실패이면 보안정책/감사부에 보고하고 결정에 따르는 과정을 포함하여 인증처리를 수행하는 것을 특징으로 하는 인증처리 장치에서의 인증처리 방법.

청구항 11. 청구항 10에 있어서,

상기 보안정책/감사부의 결정에 따르는 과정에서 결정된 정책이 임시 비밀키 갱신이면, 난수형태의 임시 비밀키를 입력으로 케이브를 수행하여 결과값인 임시 비밀키를 만들고, 단말기 상태를 임시 비밀키 갱신중으로 세팅하는 과정과;

임시 비밀키 갱신시 유일시도의 연달은 수행을 위해 난수를 입력으로 케이브를 수행하여 결과값 인증응답을 생성한 후, 단말기 상태를 유일시도중으로 세팅하는 과정과;

상기 과정 후 보안정책/감사부에서 정한 정책에 카운트 변경이 있는지 여부를 판별하여 이에 해당하는 처리를 하는 과정을 포함하여 인증처리를 수행하는 것을 특징으로 하는 인증처리 장치에서의 인증처리 방법.

청구항 12. 청구항 10에 있어서,

상기 보안정책/감사부의 결정에 따르는 과정에서 결정된 정책이 유일시도 요구이면, 난수를 입력으로 케이브를 수행하여 결과값 인증응답을 생성한 후, 단말기 상태를 유일시도중으로 세팅하는 과정과;

상기 과정 후 보안정책/감사부에서 정한 정책에 카운트 변경이 있는지 여부를 판별하여 이에 해당하는 처리를 하는 과정을 포함하여 인증처리를 수행하는 것을 특징으로 하는 인증처리 장치에서의 인증처리 방법.

청구항 13. 청구항 11 또는 청구항 12에 있어서,

보안정책/감사부에서 정한 정책에 카운트 변경 요구가 있으면, 카운트 증가에 필요한 작업을 수행하고 단말기 상태를 카운트 갱신중으로 세팅하는 과정과;

상기 과정 후 발생된 인증 실패 보고에 대한 응답을 HLR로 송신한 후, 단말기 상태가 세팅되어 있는지 판별하는 과정과;

판별 결과 세팅되어 있으면 인증상태 관리를 요청한 다음 종료하고, 그렇지 않으면 곧바로 종료하는 과정을 포함하여 인증처리를 수행하는 것을 특징으로 하는 인증처리 장치에서의 인증처리 방법.

청구항 14. 청구항 1에 있어서,

상기 인증 상태 관리 과정은, 인증처리 기능, 인증실패처리 기능 및 인증상태 변경 기능으로 부터 인증상태 관리 요구가 수신되면 해당 가입자에 대한 타이머를 설정하고 HLR로 부터 인증상태보고를 수신할때까지 기다리는 과정과;

타이머가 끝날때까지 수신되지 않으면, 단말기 상태를 확인하여 단말기 상태가 임시 비밀키 갱신중이면 새로운 임시 비밀키로 사용할 계획이던 임시 비밀키를 삭제하고, 이어 단말기 상태를 리셋한 후 보안정책/감사부에 보고한 다음 결정에 따르는 과정과;

상기 판단 결과 단말기 상태가 임시 비밀키 갱신중이 아니면 나머지 단말기 상태를 모두 리셋하고 보안정책/감사부에 보고한 후 결정에 따르는 과정과;

상기 과정에서 HLR로 부터 인증상태보고가 수신되면 단말기 상태를 모두 리셋하고 보고 목적에 따라 작업을 수행하는 과정과;

상기에서 보고 목적이 임시 비밀키 변경 성공이면 현재 임시 비밀키를 새로운 임시 비밀키로 변경하고, 임시 비밀키 변경 실패이면 보안정책/감사부에 보고한 후 다음 결정에 따르는 과정과;

상기에서 보고 목적이 카운트 변경 성공이면 인증장치 내의 해당 가입자 카운트를 증가시키고, 카운트 변경 실패이면 보안정책/감사부에 보고하고 다음 결정에 따르는 과정; 및

상기에서 보고 목적이 유일시도 성공이면 보안정책/감사부가 정해놓은 정책을 확인하고, 유일시도 실패이면 보안정책/감사부에 보고하고 다음 결정에 따르는 과정을 포함하여 인증처리를 수행하는 것을 특징으로 하는 인증처리 장치에서의 인증처리 방법.

청구항 15. 청구항 14에 있어서,

상기 보안정책/감사부에서 정한 정책이 임시 비밀키 갱신이면, 난수형태의 임시 비밀키를 입력으로 케이브를 수행하여 결과값인 임시 비밀키를 만들고 단말기 상태를 임시 비밀키 갱신중으로 세팅하는 과정과;

임시 비밀키 갱신시 유일시도의 연달은 수행을 위해 난수를 입력으로 케이브를 수행하여 결과값 인증응답을 생성한 후, 단말기 상태를 유일시도중으로 세팅하는 과정과;

상기 과정 후 보안정책/감사부에서 정한 정책에 카운트 변경이 있는지 여부를 판별하여 이에 해당하는 처리를 하는 과정을 포함하여 인증처리를 수행하는 것을 특징으로 하는 인증처리 장치에서의 인증처리 방법.

청구항 16. 청구항 14에 있어서,

한편, 보안정책/감사부가 정한 정책이 유일시도 요구이면(09) 난수를 입력으로 케이브를 수행하여 결과값인 인증응답을 생성한 후, 단말기 상태를 유일시도중으로 세팅한다(091).

상기 과정 후 보안정책/감사부에서 정한 정책에 카운트 변경이 있는지 여부를 판별하여 이에 해당하는 처리를 하는 과정을 포함하여 인증처리를 수행하는 것을 특징으로 하는 인증처리 장치에서의 인증처리 방법.

청구항 17. 청구항 15 또는 청구항 16에 있어서,

보안정책/감사부에서 정한 정책에 카운트 변경 요구가 있으면, 카운트 증가에 필요한 작업을 수행하고 단말기 상태를 카운트 갱신중으로 세팅하는 과정과;

상기 과정 후 발생된 인증 실패 보고에 대한 응답을 HLR로 승신한 후, 단말기 상태가 세팅되어 있는지 판별하는 과정과;

판별결과 단말기 상태가 세팅되어 있으면 다시 타이머를 설정하고 대기 상태로 전환하는 과정을 반복 수행하는 과정을 포함하여 인증처리를 수행하는 것을 특징으로 하는 인증처리 장치에서의 인증처리 방법.

청구항 18. 청구항 1에 있어서,

상기 망 인증 처리 과정은, 상기 분배 기능으로 부터 망인증 요구가 수신되면 기지국 시도용 난수를 입력으로 케이브를 수행한 후, 결과값인 기지국 인증응답을 생성하는 과정과;

이어 상기 생성된 기지국 응답을 승신한 후 종료하는 과정을 포함하여 인증처리를 수행하는 것을 특징으로 하는 인증처리 장치에서의 인증처리 방법.

청구항 19. 청구항 1에 있어서,

상기 인증상태변경 처리 과정은, 보안정책/감사부가 인증상태변경 결정을 내려 인증상태변경 기능이 요구되면 보안정책/감사부의 결정이 무엇인지를 판단하는 과정과;

상기 판단 결과 보안정책/감사부가 정한 정책이 임시 비밀키 갱신이면, 이에 해당하는 처리를 수행하는 과정과;

상기 판단 결과 보안정책/감사부가 정한 정책이 유일시도 요구이면, 난수를 입력으로 케이브를 수행하여 결과값 인증응답을 생성한 후, 단말기 상태를 유일시도중으로 세팅하는 과정과;

상기 각 임시 비밀키 갱신 또는 유일시도 처리 후 보안정책/감사부가 정한 정책에 카운트 변경이 있는지 검사하여 요구하는 경우, 카운트 증가에 필요한 작업을 수행하고 단말기 상태를 카운트 갱신중으로 세팅하는 과정과;

이어 인증상태변경 요구를 HLR로 승신한 후 결과를 기다리는 과정과;

인증상태변경 결과가 HLR로 부터 수신되면 실패 및 성공 여부를 판단하여 판단 결과에 해당하는 처리를 수행하는 과정을 포함하여 인증처리를 수행하는 것을 특징으로 하는 인증처리 장치에서의 인증처리 방법.

청구항 20. 청구항 19에 있어서,

상기 판단결과 성공인 경우 처리 과정은 단말기 상태가 세팅되어 있는지 검사하여, '임시 비밀키 갱신중', '유일시도중', '카운트 갱신중' 중 하나라도 세팅되어 있으면 인증상태 관리를 요구하고 종료하는 과정을 포함하여 인증처리를 수행하는 것을 특징으로 하는 인증처리 장치에서의 인증처리 방법.

청구항 21. 청구항 19에 있어서,

상기 판단 결과 실패인 경우 처리 과정은 단말기 상태가 '임시 비밀키 갱신중'인 경우에만 새로 발생시켜 놓았던 임시 비밀키를 삭제하고, 나머지 경우에는 단말기 상태만 리셋한 후 인증처리 장치 내에서 가입자의 인증상태를 변경전 상태로 만들어 놓기 위한 처리를 수행한 후 종료하는 과정을 포함하여 인증처리를 수행하는 것을 특징으로 하는 인증처리 장치에서의 인증처리 방법.

청구항 22. 청구항 19에 있어서,

상기 임시 비밀키 갱신 처리를 수행하는 과정은 난수용 임시 비밀키를 입력으로 케이브를 수행하여 결과값인 임시 비밀키를 만들고, 이어 단말기 상태를 임시 비밀키 갱신중으로 세팅하는 과정과;

임시 비밀키 갱신시 유일시도의 연달은 수행을 위해, 난수를 입력으로 케이브를 수행하여 결과값 인증응답을 생성한 후, 단말기 상태를 유일시도중으로 세팅하는 과정을 포함하여 인증처리를 수행하는 것을 특징으로 하는 인증처리 장치에서의 인증처리 방법.

청구항 23. 청구항 1에 있어서,

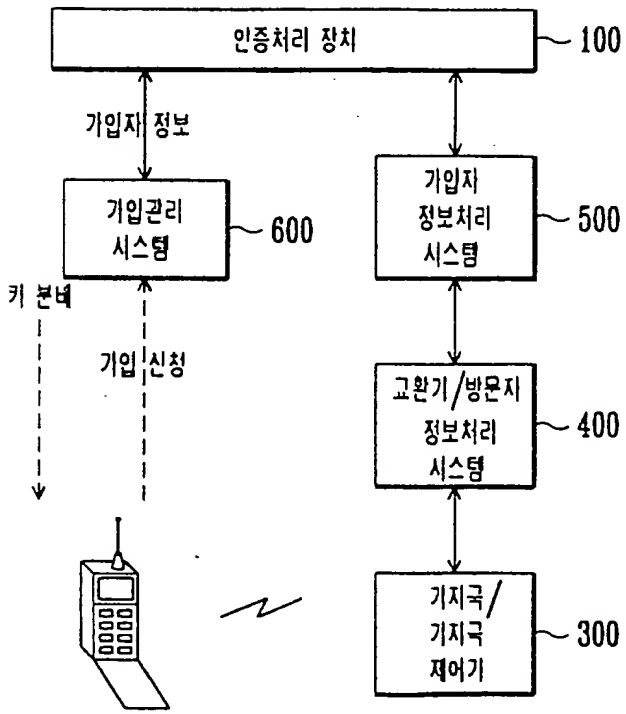
상기 인증관련처리트래픽 수집 기능의 처리 과정은, 평상시 대기 상태로 관련 트래픽을 수집하는 과정과;

상기 과정에서 내부 기능들로 부터 인증관련 처리 트래픽 정보가 수신되면 관리하고 있던 해당 트래픽 항목을 증가시킨 후 종료하는 과정과;

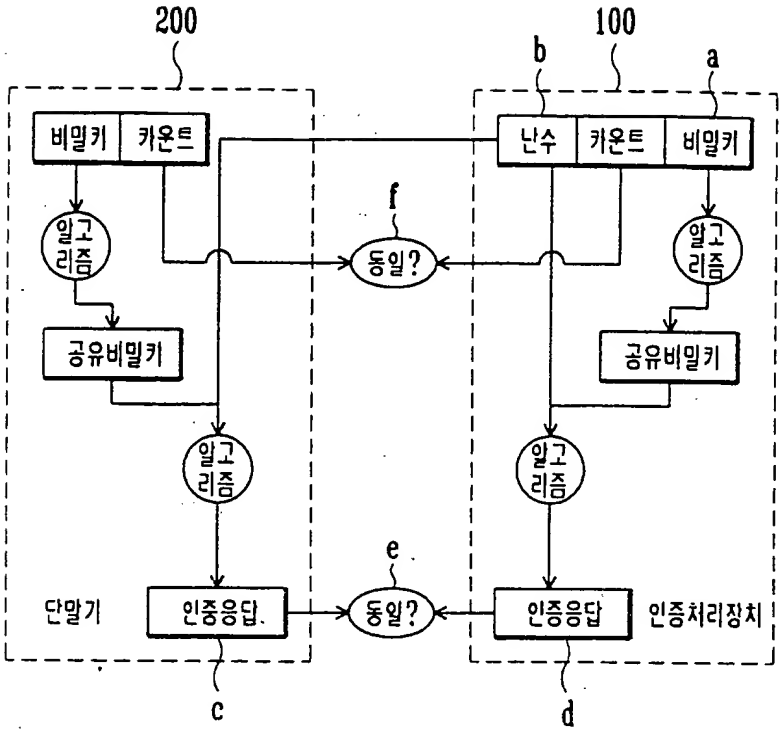
상기 과정에서 운용관리부로 부터 관리하던 트래픽 정보 요구가 수신되면 해당 항목의 현재값을 운용관리 장치로 송신하고, 관리하던 항목값은 리셋하는 과정을 포함하여 인증처리를 수행하는 것을 특징으로 하는 인증처리 장치에서의 인증처리 방법.

도면

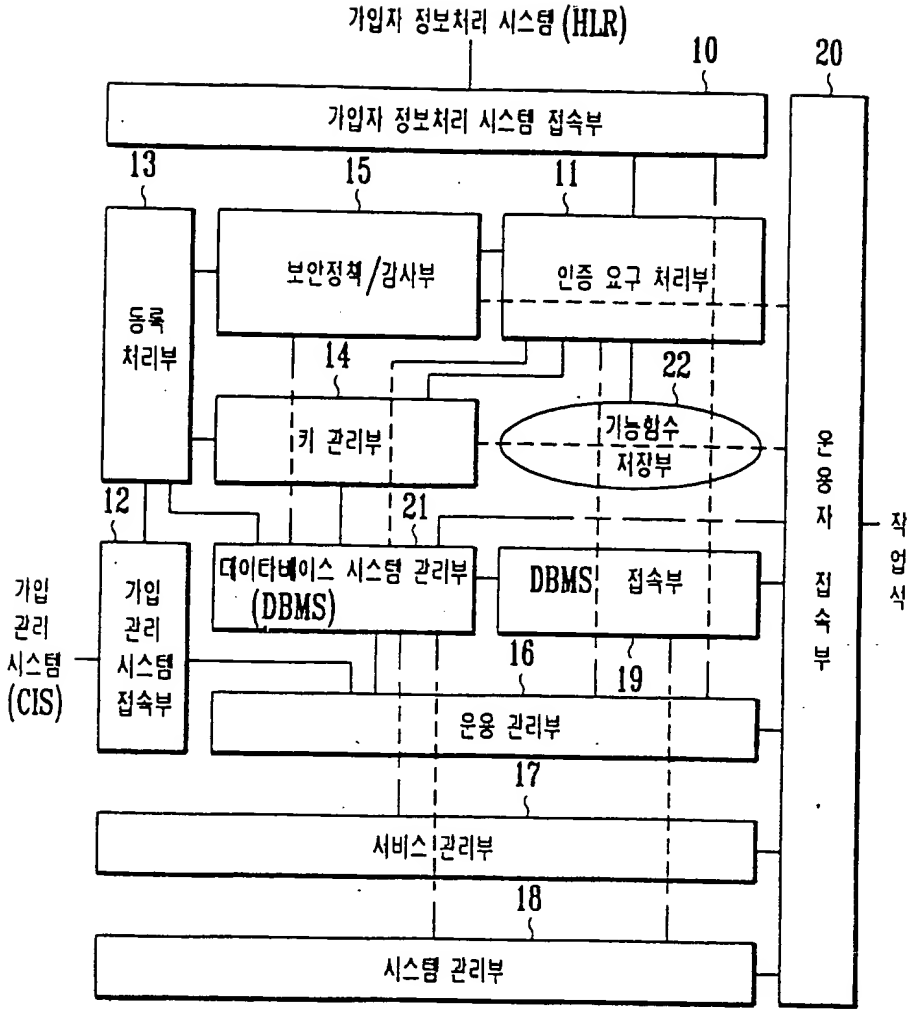
도면1



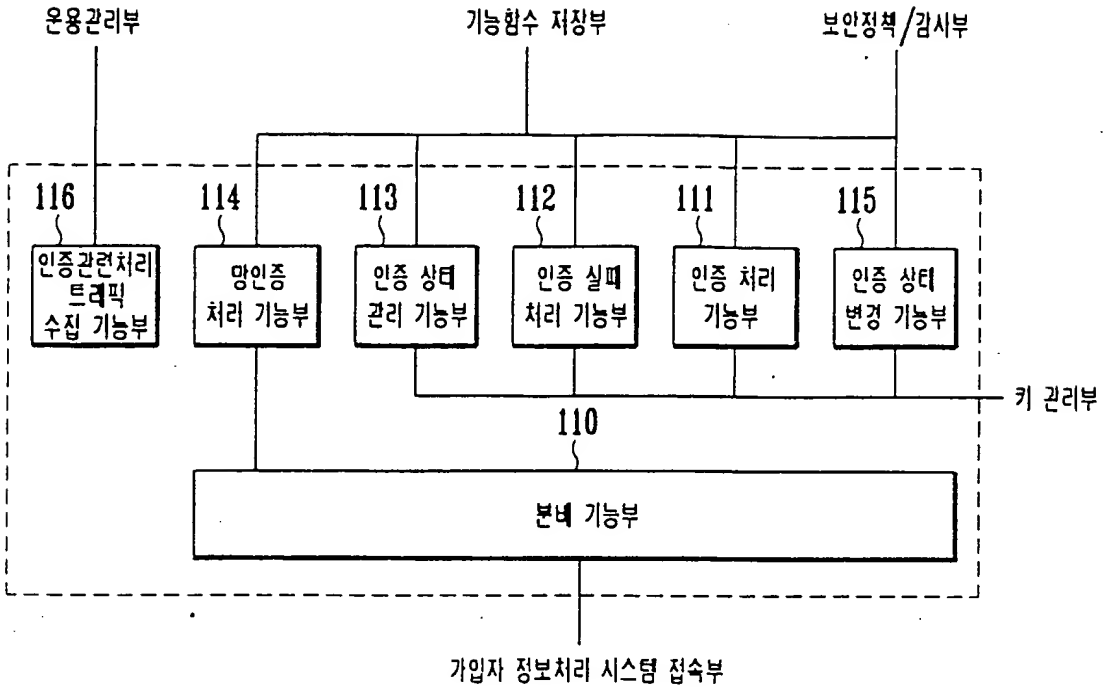
도면2


200
100
b
a
비밀키
카운트
난수
카운트
비밀키
f
알고리즘
동일?
알고리즘
공유비밀키
공유비밀키
알고리즘
알고리즘
e
단말기
인증응답
동일?
인증응답
인증처리장치
c
d

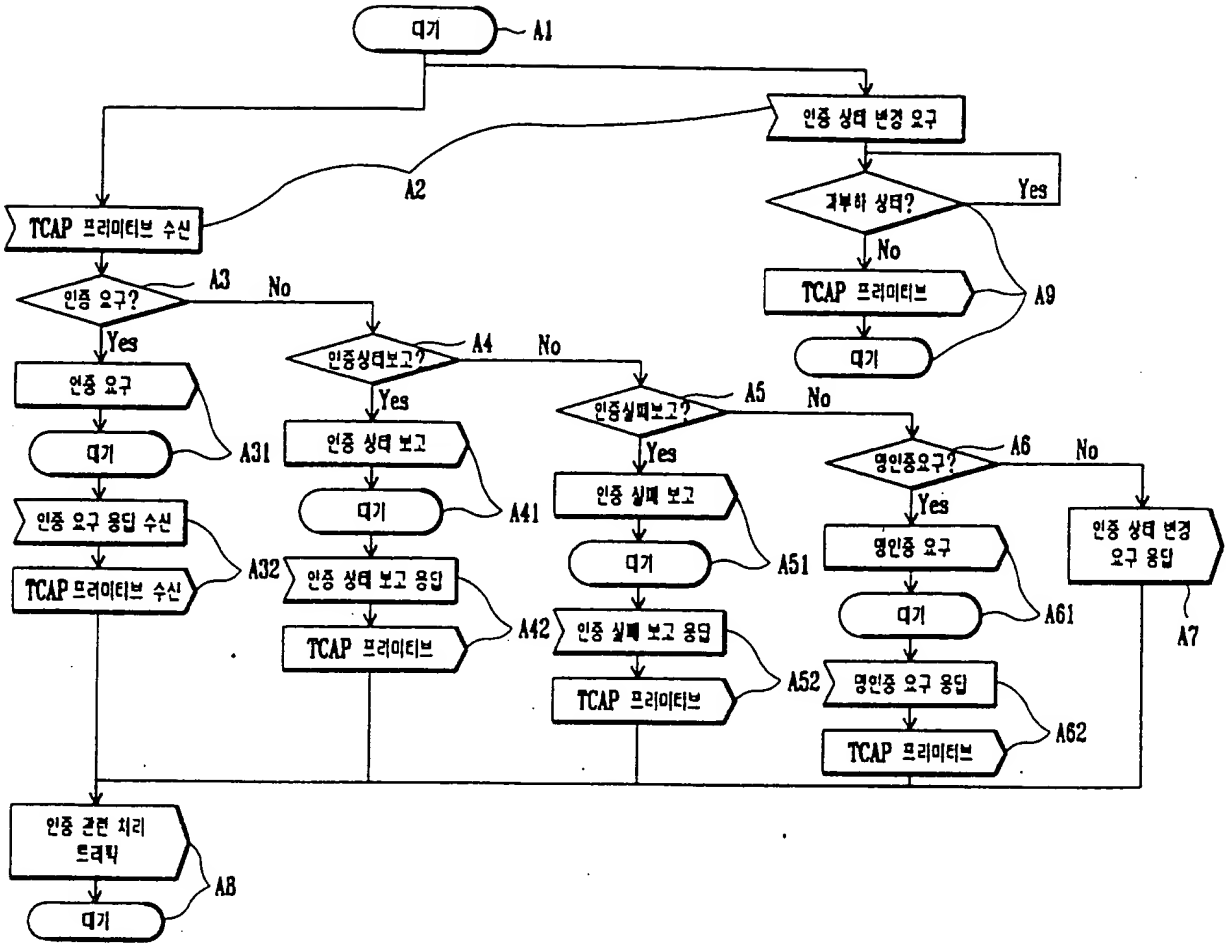
도면3


가입자 정보처리 시스템 (HLR)
10
20
가입자 정보처리 시스템 접속부
13
15
11
동록 처리부
보안정책/감사부
인증 요구 처리부
14
22
키 관리부
기능함수 저장부
12
21
가입 관리 시스템 (CIS)
가입 관리 시스템 접속부
데이타베이스 시스템 관리부 (DBMS)
DBMS 접속부
16
19
운용 관리부
17
서비스 관리부
18
시스템 관리부
운용자 접속부
작업식

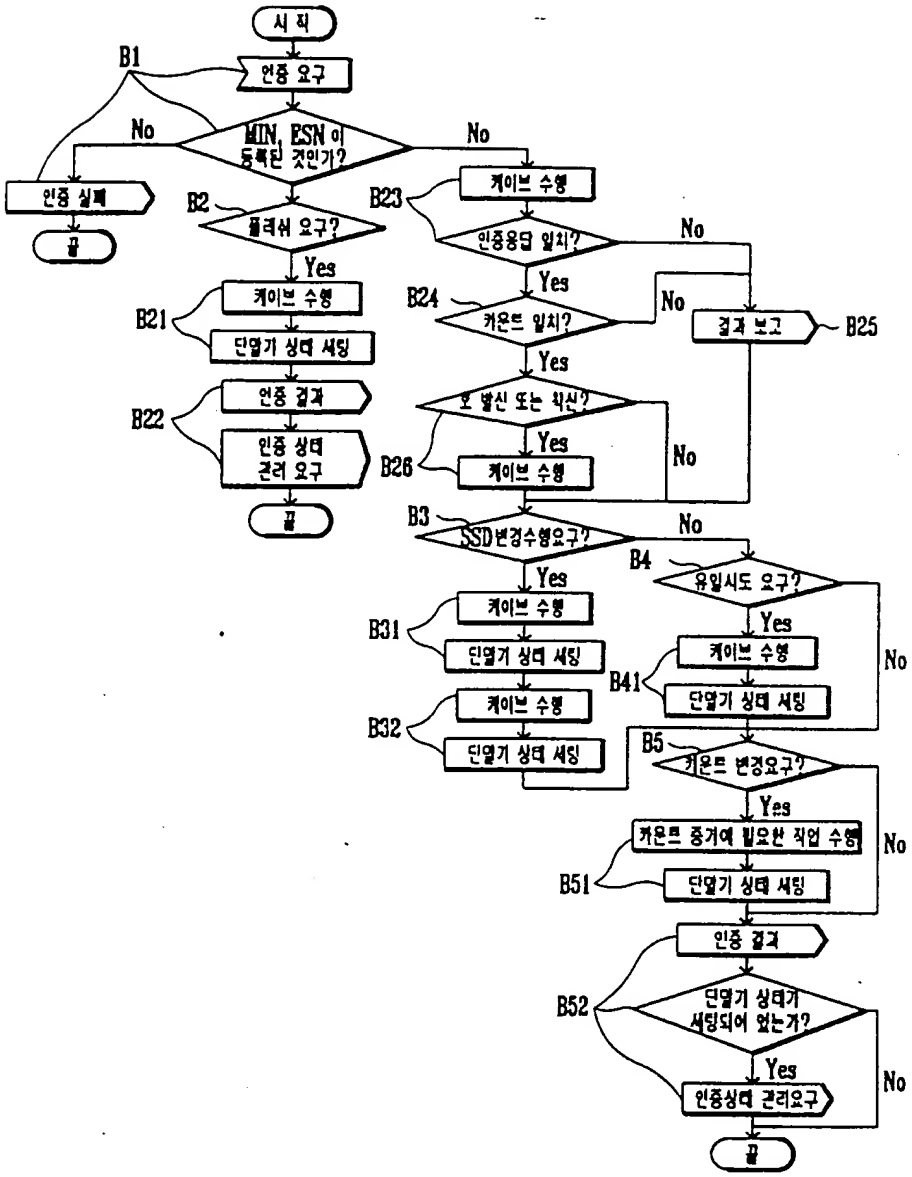
도면4


운용관리부
기능함수 저장부
보안정책/감시부
116
114
113
112
111
115
인증관련처리 트래픽 수집 기능부
망인증 처리 기능부
인증 상태 관리 기능부
인증 실패 처리 기능부
인증 처리 기능부
인증 상태 변경 기능부
키 관리부
110
본체 기능부
가입자 정보처리 시스템 접속부

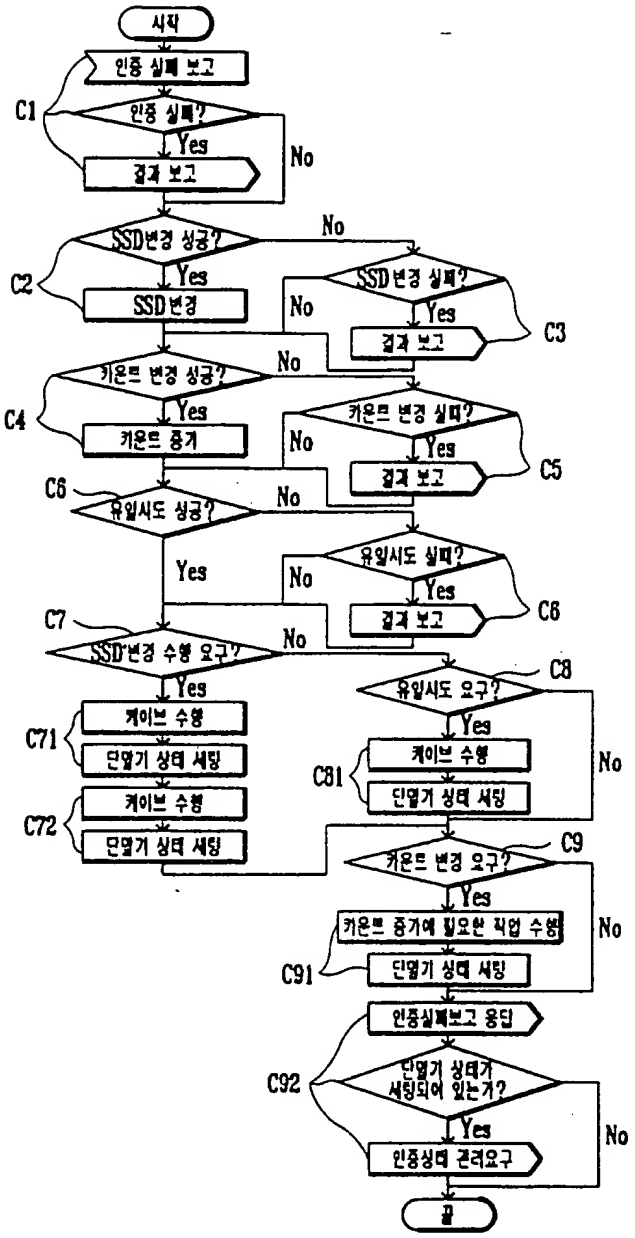
도면5


대기
A1
인증 상태 변경 요구
A2
TCAP 프리미티브 수신
과부하 상태?
Yes
No
TCAP 프리미티브
A9
대기
인증 요구?
A3
No
Yes
인증상태보고?
A4
No
인증 요구
대기
A31
인증 상태 보고
Yes
인증실패보고?
A5
No
명인증요구?
A6
No
Yes
인증 요구 응답 수신
TCAP 프리미티브 수신
A32
대기
A41
인증 실패 보고
대기
A51
명인증 요구
대기
A61
인증 상태 보고 응답
TCAP 프리미티브
A42
인증 실패 보고 응답
TCAP 프리미티브
A52
명인증 요구 응답
TCAP 프리미티브
A62
인증 상태 변경 요구 응답
A7
인증 관련 처리 트랙킹
A8
대기

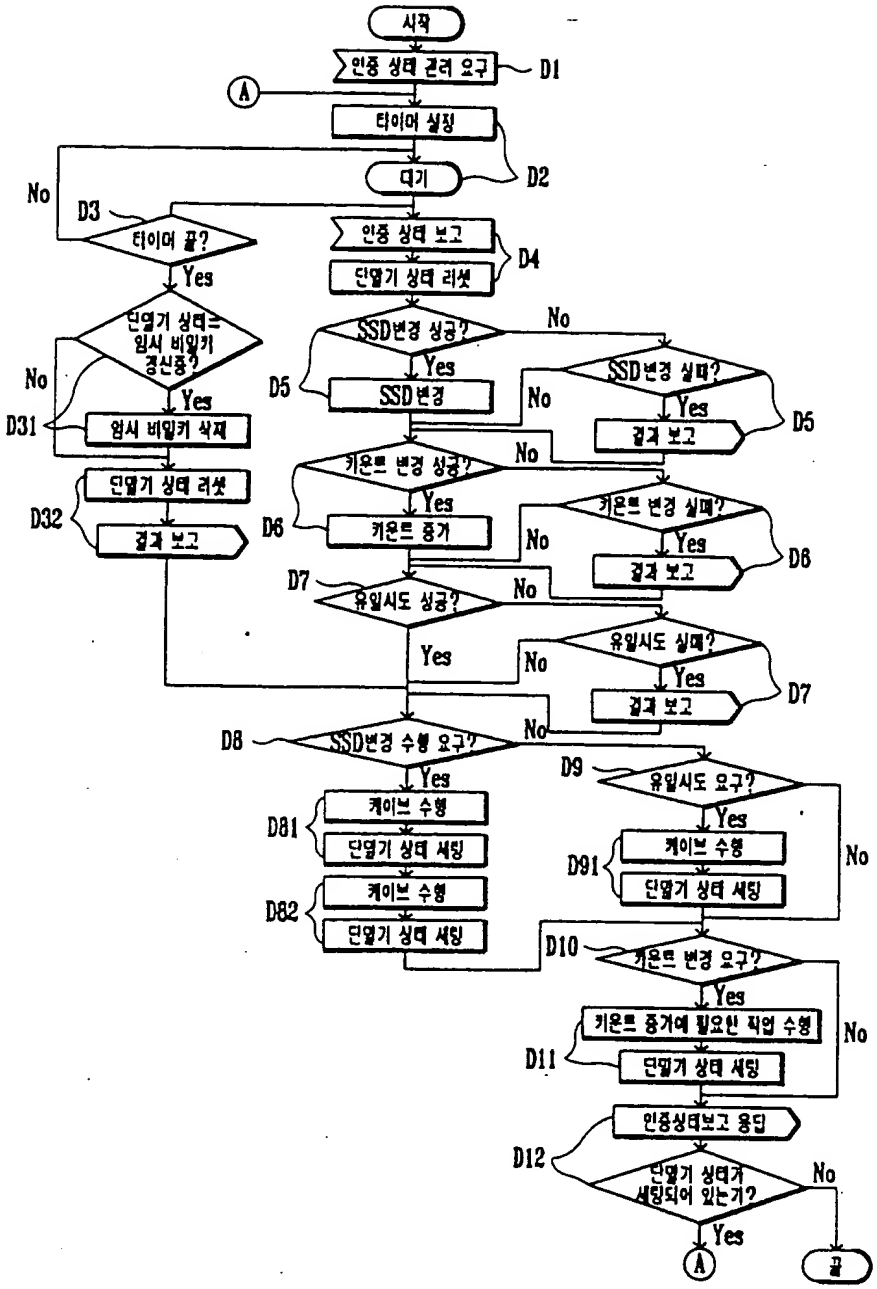
도면6


시 작
B1
인증 요구
No
MIN, ESN 이 등록된 것인가?
No
인증 실패
끝
B2
플러쉬 요구?
Yes
B21
케이브 수행
단말기 상태 세팅
B22
인증 결과
인증 상태 관리 요구
끝
B23
케이브 수행
인증응답 일치?
No
Yes
B24
카운트 일치?
No
결과 보고
B25
Yes
호 발신 또는 착신?
Yes
B26
케이브 수행
No
B3
SSD변경수행요구?
No
Yes
B31
케이브 수행
단말기 상태 세팅
B32
케이브 수행
단말기 상태 세팅
B4
유일시도 요구?
Yes
No
B41
케이브 수행
단말기 상태 세팅
B5
카운트 변경요구?
Yes
No
B51
카운트 증가에 필요한 작업 수행
단말기 상태 세팅
B52
인증 결과
단말기 상태가 세팅되어 있는가?
Yes
No
인증상태 관리요구
끝

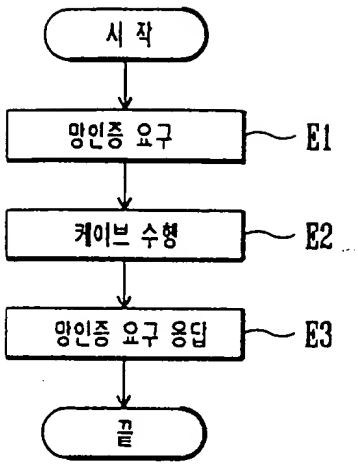
도면7


시작
인증 실패 보고
C1
인증 실패?
Yes
No
결과 보고
SSD변경 성공?
No
C2
Yes
SSD변경
SSD변경 실패?
No
Yes
결과 보고
C3
키온트 변경 성공?
No
C4
Yes
키온트 증가
키온트 변경 실패?
No
Yes
결과 보고
C5
C6
유일시도 성공?
No
Yes
유일시도 실패?
No
Yes
결과 보고
C6
C7
SSD변경 수행 요구?
No
Yes
C8
유일시도 요구?
Yes
No
C71
케이브 수행
단말기 상태 세팅
C72
케이브 수행
단말기 상태 세팅
C81
케이브 수행
단말기 상태 세팅
C9
키온트 변경 요구?
Yes
No
키온트 증가에 필요한 작업 수행
C91
단말기 상태 세팅
인증실패보고 응답
C92
단말기 상태가 세팅되어 있는가?
Yes
No
인증상태 관련요구
끝

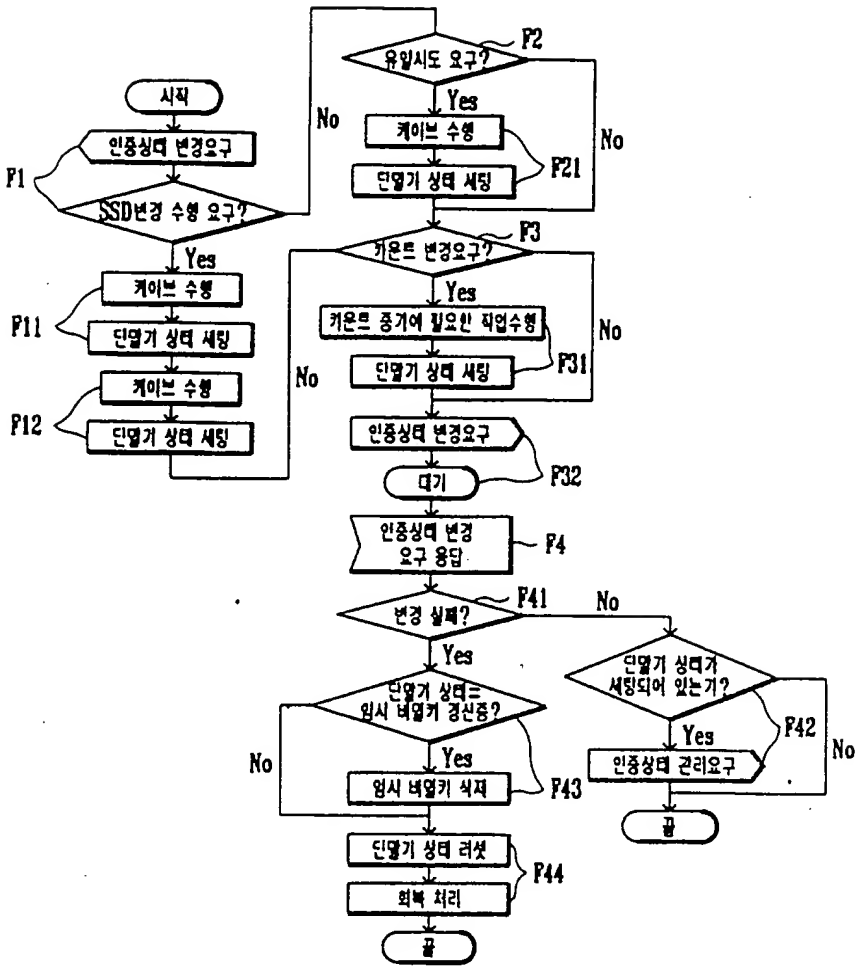
도면8


시작
인증 상태 관리 요구
D1
A
타이머 설정
대기
D2
No
D3
타이머 끝?
Yes
인증 상태 보고
단말기 상태 리셋
D4
단말기 상태는 임시 비밀키 갱신중?
No
Yes
D31
임시 비밀키 삭제
단말기 상태 리셋
D32
결과 보고
SSD변경 성공?
No
Yes
D5
SSD변경
SSD변경 실패?
No
Yes
결과 보고
D5
키온트 변경 성공?
No
Yes
D6
키온트 증거
키온트 변경 실패?
No
Yes
결과 보고
D6
D7
유일시도 성공?
No
Yes
유일시도 실패?
No
Yes
결과 보고
D7
D8
SSD변경 수행 요구?
No
Yes
D9
유일시도 요구?
Yes
No
D81
케이브 수행
단말기 상태 세팅
D82
케이브 수행
단말기 상태 세팅
D91
케이브 수행
단말기 상태 세팅
D10
키온트 변경 요구?
Yes
No
키온트 증거에 필요한 작업 수행
D11
단말기 상태 세팅
인증상태보고 응답
D12
단말기 상태가 세팅되어 있는가?
No
Yes
A
끝

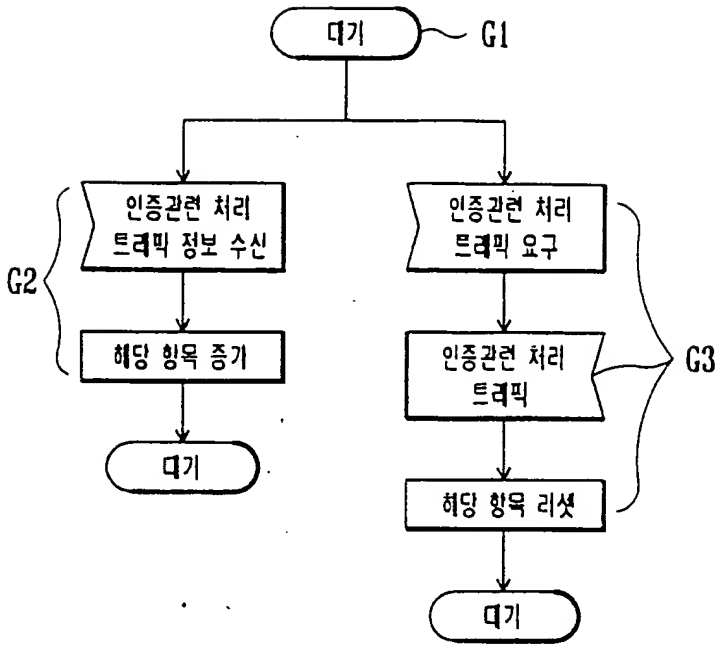
도면9



도면10


시작
인증상태 변경요구
F1
SSD변경 수행 요구?
No
Yes
케이브 수행
F11
단말기 상태 세팅
케이브 수행
F12
단말기 상태 세팅
No
유입시도 요구?
P2
Yes
케이브 수행
No
단말기 상태 세팅
P21
키온르 변경요구?
P3
Yes
키온르 증기어 필요한 작업수행
No
단말기 상태 세팅
P31
인증상태 변경요구
대기
P32
인증상태 변경 요구 응답
P4
변경 실패?
P41
No
Yes
단말기 상태= 임시 비멀키 경신중?
No
Yes
임시 비멀키 삭제
P43
단말기 상태 리셋
P44
회복 처리
끝
단말기 상태가 세팅되어 있는가?
P42
Yes
No
인증상태 관리요구
끝

도면11


대기
G1
인증관련 처리
트래픽 정보 수신
G2
해당 항목 증가
대기
인증관련 처리
트래픽 요구
인증관련 처리
트래픽
G3
해당 항목 리셋
대기